



Perform Configuration Audits Using Compliance

- [How To Perform a Compliance Audit, on page 1](#)
- [Enable and Disable Compliance Auditing, on page 2](#)
- [Create a New Compliance Policy, on page 2](#)
- [Create Compliance Policy Rules, on page 3](#)
- [Create a Compliance Profile That Contains Policies and Rules, on page 5](#)
- [Run a Compliance Audit, on page 6](#)
- [View the Results of a Compliance Audit, on page 7](#)
- [View Violation Job Details, on page 8](#)
- [View Change Audit Details, on page 8](#)
- [View Audit Failure and Violation Summary Details, on page 8](#)
- [Fix Device Compliance Violations, on page 9](#)
- [View Audit Failure and Violation Summary Details, on page 10](#)
- [Import and Export Compliance Policies, on page 11](#)
- [View the Contents of a Compliance Policy XML File, on page 11](#)
- [View PSIRT and EoX Information, on page 11](#)

How To Perform a Compliance Audit

The following table lists the basic steps for using the Compliance feature.

	Description	See:
1	Create a <i>compliance policy</i> that contains a name and other descriptive text.	Create a New Compliance Policy, on page 2
2	Add rules to the compliance policy. The rules specify what constitutes a violation.	Create Compliance Policy Rules, on page 3

3	<p>Create a <i>compliance profile</i> (which you will use to run an audit on network devices) and:</p> <ul style="list-style-type: none"> • Add a compliance policy to it. • Choose the policy rules you want to include in the audit. <p>You can add multiple custom policies and/or predefined system policies to the same profile.</p>	Create a Compliance Profile That Contains Policies and Rules, on page 5
4	Run a compliance audit by selecting a profile and scheduling an audit job.	Run a Compliance Audit, on page 6
5	View the results of the compliance audit and if necessary, fix the violations.	View the Results of a Compliance Audit, on page 7

Enable and Disable Compliance Auditing

The Compliance feature uses device configuration baselines and audit policies to find and correct any configuration deviations in network devices. It is disabled by default because some of the compliance reports can impact system performance. To enable the Compliance feature, use the following procedure.

-
- Step 1** Choose **Administration > Settings > System Settings**, then choose **General > Server**.
- Step 2** Next to Compliance Services, click **Enable**, then click **Save**.
- Step 3** Re-synchronize Cisco EPN Manager's device inventory: Choose **Inventory > Network Devices**, select all devices, then click **Sync**.
- Step 4** Logout of Cisco EPN Manager and login again to view Compliance under the **Configuration** tab.
- If you still don't see the different Compliance options under the Configuration tab, ensure that you have the required system requirements as explained in the latest [Cisco Evolved Programmable Network Manager Installation Guide](#).
-

Create a New Compliance Policy

You can create a new compliance policy starting with a blank policy template.

-
- Step 1** Choose **Configuration > Compliance > Policies**.
- Step 2** Click the Create Compliance Policy (+) icon in the **Compliance Policies** navigation area on the left.
- Step 3** In the dialog box, enter a name and optional description, then click **Create**. The policy is added to the **Compliance Policies** navigation area on the left.
- To duplicate the policy click the **i** icon and choose **Duplicate Policy**.
-

What to do next

Add rules to the compliance policy. See [Create Compliance Policy Rules, on page 3](#).

Create Compliance Policy Rules

Compliance policy rules are platform-specific and define what is considered a device violation. A rule can also contain CLI commands that fix the violation. When you are designing the compliance audit job, you can select the rules you want to include in the audit (see [Run a Compliance Audit, on page 6](#)).

Cisco EPN Manager supports audit for AireOS Wireless LAN Controllers platform.

Step 1 Choose **Configuration > Compliance > Policies**, then select a policy from the navigation area on the left.

Step 2 From the work area pane, click **New** to add a new rule.

If a similar rule exists, you can copy the rule by clicking **Duplicate**, editing the rule, and saving it with a new name.

Step 3 Configure the new rule by entering your rule criteria.

Note Cisco EPN Manager supports all Java-based regular expressions. See <http://www.rexegg.com/regex-quickstart.html>.

- a) Enter a title, description, and other information in the **Rule Information** text fields. This information is free text and does not impact any of the rule settings.
- b) Specify the devices for this rule in the **Platform Selection** area.
- c) (Optional) In the **Rule Inputs** area, click **New** and specify the input fields that should be displayed to a user when they run a policy that contains this rule. For example, you could prompt a user for an IP address.

Note If you choose the **Accept Multiple Values** check box, the audit will pass only if all the rule inputs match in the condition.

- d) In the **Conditions and Actions** area, click **New** and specify the criteria that will be checked. This will determine the rule pass and fail conditions. For examples, see [Examples—Rule Conditions and Actions, on page 3](#).

Step 4 Click **Create**. The rule is added to the compliance policy.

You can create as many rules as you want. Remember that when you want to run the audit job, you can pick the rules you want to validate.

What to do next

Create a profile that contains the compliance policy and its rules, and then perform the audit using the profile. See [Create a Compliance Profile That Contains Policies and Rules, on page 5](#).

Examples—Rule Conditions and Actions

- [Example Conditions and Actions: DNS Servers Configured on Device, on page 4](#)
- [Example Conditions and Actions: Community Strings, on page 4](#)
- [Example Conditions and Actions: IOS Software Version, on page 4](#)
- [Example Conditions and Actions: NTP Server Redundancy, on page 5](#)

Example Conditions and Actions: DNS Servers Configured on Device

This compliance policy checks if either **IP name-server 1.2.3.4** or **IP name-server 2.3.4.5** is configured on the device. If they are, the policy raises a violation with the message "DNS server must be configured as either 1.2.3.4 or 2.3.4.5."

Tab	Tab Area	Field	Value
Condition Details	Condition Scope Details	Condition Scope	Configuration
	Condition Match Criteria	Operator	Matches the expression
		Value	ip name-server {1.2.3.4 2.3.4.5}
Action Details	Select Match Action	Select Action	Does not raise a violation
	Select Does Not Match Action	Select Action	Raise a violation
		Violation Message Type	User Defined Violation Message
		Violation Text	DNS server must be configured as either 1.2.3.4 or 2.3.4.5

Example Conditions and Actions: Community Strings

This compliance policy checks if either **snmp-server community public** or **snmp-server community private** is configured on a device (which is undesirable). If it is, the policy raises a violation with the message "Community string xxxxx configured", where xxx is the first violation that was found.

Tab	Tab Area	Field	Value
Condition Details	Condition Scope Details	Condition Scope	Configuration
	Condition Match Criteria	Operator	Matches the expression
		Value	snmp-server community {public private}
Action Details	Select Match Action	Select Action	Raise a violation
	Select Does Not Match Action	Select Action	Continue
		Violation Message Type	User Defined Violation Message
		Violation Text	Community string xxxxx configured.

Example Conditions and Actions: IOS Software Version

This compliance policy checks if Cisco IOS software version **15.0(2)SE7** is installed on a device. If it is not, the policy raises a violation with the message "Output of show version contains the string xxxxx," where xxxxx is the Cisco IOS software version that does not match 15.0(2)SE7.

Tab	Tab Area	Field	Value
Condition Details	Condition Scope Details	Condition Scope	Device Command Outputs
		Show Commands	show version
	Condition Match Criteria	Operator	Contains the string
		Value	15.0(2)SE7
Action Details	Select Match Action	Select Action	Continue
	Select Does Not Match Action	Select Action	Raise a Violation
		Violation Message Type	User Defined Violation Message
		Violation Text	Output of show version contains the string xxxxx.

Example Conditions and Actions: NTP Server Redundancy

This compliance policy checks if the command **ntp server** appears at least twice on the device. If it does not, the policy raises a violation with the message "At least two NTP servers must be configured."

Tab	Tab Area	Field	Value
Condition Details	Condition Scope Details	Condition Scope	Configuration
	Condition Match Criteria	Operator	Matches the expression
		Value	(ntp server.*\n){2,}
Action Details	Select Match Action	Select Action	Continue
	Select Does Not Match Action	Select Action	Raise a violation
		Violation Message Type	User Defined Violation Message
		Violation Text	At least two NTP servers must be configured.

Create a Compliance Profile That Contains Policies and Rules

A compliance profile contains one or more compliance policies. When you add a compliance policy to a profile, all of the policy's rules are applied to the profile. You can customize the profile by selecting the policy rules you want to include (and ignoring the others). If you group several policies in a profile, you can select and deselect the rules for each policy.

Step 1 Choose **Configuration > Compliance > Profiles**.

- Step 2** Click the Create Policy Profile (+) icon in the **Compliance Profiles** navigation area on the left. This opens the **Add Compliance Policies** dialog box.
- Step 3** Select the policies you want to include in the profile. User defined policies will be available under the User Defined category.
- In the **Add Compliance Policies** dialog box, choose the policies you want to add.
 - Click **OK**. The policies are added to the **Compliance Policy Selector** area.
- Step 4** Select the rules you want to include in the policy.
- Select a policy in the **Compliance Policy Selector** area. The policy's rules are displayed in the area on the right.
 - Select and deselect specific rules, then click **Save**.
- Note** The choices you make here only apply to the *policy instance in this profile*. Your choices do not modify the original version of the compliance policy.

What to do next

Schedule the compliance audit job as described in [Run a Compliance Audit, on page 6](#).

Run a Compliance Audit

To run a compliance audit, select a profile, choose the devices you want to audit (using the policies and rules in the profile), and schedule the audit job.

- Step 1** Choose **Configuration > Compliance > Profiles**.
- Step 2** Select a profile in the **Compliance Profiles** navigation area on the left.
- Step 3** Click the Run Compliance Audit icon in the **Compliance Profiles** navigation area.
- Step 4** Expand the **Devices and Configuration** area, select the required devices and configuration files that you want to audit.
- Select the devices (or device groups).
 - Specify which configuration file you want to audit.
 - **Use Latest Archived Configuration** —Audit the latest backup file from the archive. If no backup file is available, Cisco EPN Manager does not audit the device.
 - **Use Current Device Configuration**— Poll and audit the device's running configuration. (For example, show command output will be from the device's running configuration.)

When you select this option, Cisco EPN Manager first takes a backup of the configuration from device and then performs audit. This is useful when periodic or event triggered configuration backup is not enabled and also useful because archived configuration in Cisco EPN Manager is often out-of-sync with the device.
 - Click **Next**.
- Step 5** Select **Now** to schedule the audit job immediately or select **Date** and enter a date and time to schedule it later.
- Use the **Reccurence** option to repeat the audit job at regular intervals.

- Step 6** Click **Finish**. An audit job is scheduled. To view the status of the audit job, choose **Configuration > Compliance > Jobs**.

What to do next

Check the audit results as described in [View the Results of a Compliance Audit, on page 7](#).

View the Results of a Compliance Audit

Use this procedure to check an audit job results. The results will tell you which devices were audited, which devices were skipped, which devices had violations, and so forth. There might be several different compliance policies running on a single device.

After a job is created, you can set the following preferences for the job:

- **Pause Series**—Can be applied only on jobs that are scheduled in the future. You cannot suspend a job that is running.
- **Resume Series**—Can be applied only on jobs that have been suspended.
- **Edit Schedule**—Reschedule a job that has been scheduled for a different time.

- Step 1** Choose **Configuration > Compliance > Jobs**.

- Step 2** Click the **Audit Jobs** tab, locate your job, and check the information in the **Last Run** column.

Last Run Result Value	Description
Failure	One or more devices audited have a violation in the policies specified in the profile.
Partial Success	The compliance job contains a mix of both audited and non-audited devices, and the compliance status of audited devices is successful.
Success	All devices audited conform to the policies specified in the profile.

For a compliance audit job, the number of violations supported is 20000 for Standard setup and 80000 for Pro and above setup of Cisco EPN Manager.

- Step 3** If the audit check failed:

- To see which devices failed, hover over the "i" icon next to the **Failure** hyperlink to display a details popup.
- Launch a Device 360 view by selecting the job, clicking **View Job Details**, and clicking the "i" icon next to a device in the popup window.

- Step 4** For the most detail, click the **Failure** hyperlink to open the **Compliance Audit Violation Details** window.

Note Use the **Next** and **Previous** buttons to traverse the **Compliance Audit Violation Details** window.

- Check the **Job Details and Violations** area for a summary of the failures. The fields are described in the section *Administration > Dashboards > Job Dashboard > User Jobs > Compliance Jobs* in [Cisco Prime Infrastructure Field Reference](#) (the content is applicable to Cisco EPN Manager).

- Check the **Violations by Device** area for per-device details.

What to do next

To fix any of the violations, see [Fix Device Compliance Violations, on page 9](#).

View Violation Job Details

The following table shows the details that can be viewed from the Violation Details page.

To View:	Do the following
The status of scheduled fixable violation jobs.	<ol style="list-style-type: none"> 1. Go to the Violation Details page. 2. Click the Fixable column filter box and choose Running.
The details of Fixed violation jobs.	<ol style="list-style-type: none"> 1. Go to the Violation Details page. 2. Click the Fixable column filter box and choose Fixed. 3. Click the Fixed link.
The details of Fix Failed violation jobs.	<ol style="list-style-type: none"> 1. Go to the Violation Details page. 2. Click the Fixable column filter box and choose Fix Failed. 3. Click the Fix Failed link.

View Change Audit Details

Step 1 Log in to Cisco EPN Manager as an administrator

Step 2 Choose **Monitor > Tools > Change Audit Dashboard**.

The **Change Audit Dashboard** displays the network audit logs and change audit data of device management, user management, configuration template management, device community and credential changes, and inventory changes of devices. The **Change Audit report** and **Change Audit** dashboard display the details irrespective of the virtual domain you are logged in.

View Audit Failure and Violation Summary Details

You can view detailed violation information, export this data, and view details of compliance jobs. You can export detailed data for a specific job, or export summary data for multiple jobs.

Step 1 Choose **Configuration > Compliance > Jobs**.

Step 2

To view the details for a specific audit job:

- a) Click the **Audit Jobs** tab and locate your job.
- b) Click the job's **Failure** hyperlink to view the **Compliance Audit Details** window.

You can view information about the policy name, the set rules, its compliance state, the total violation count, the job's instance count, its highest severity value, and the ignored count values.

- c) To export these details use one of the following options:
 - To export the violation details to a Microsoft Excel spreadsheet in XLS format, click **Export as XLS**.
 - To export the violation details to a Microsoft Excel spreadsheet in comma-separated text, click **Export as CSV**.
 - To export the violation details to an HTML file, click **Export as HTML**.
- d) Click **Save File**.

Step 3

To view a collective summary of all audit jobs:

- a) Click the **Violation Summary** tab.

You can view a collective report for all devices on which violations have occurred, their associated policy and profile names, their audit job IDs, their associated rules and rule severity values, details on whether the violations are fixable or not, or whether they are already fixed, and the message associated with the violation.

- b) To export this detailed summary report, choose one of the following options from the drop-down menu:
 - To export the summary to a Microsoft Excel spreadsheet in comma-separated text, click **Violation Report CSV**.
 - To export the summary to a PDF file, click **Violation Report PDF**.
- c) Click **Save File**.

What to do next

To fix any of the violations, see [Fix Device Compliance Violations, on page 9](#).

Fix Device Compliance Violations

Use this procedure to fix compliance violations for a failed compliance audit.

Step 1

Choose **Configuration > Compliance > Jobs**.

Step 2

Click the **Audit Jobs**, locate your job, and check the information in the **Last Run Result** column.

Step 3

Click the **Failure** hyperlink to open the **Compliance Audit Violation Details** window.

Note Use the **Next** and **Previous** buttons to traverse the **Compliance Audit Violation Details** window.

Step 4

In the **Job Details and Violations** area, click **Next**.

Step 5

In the **Violations by Device** area, select the device and violation and click **Next**.

Step 6

In the **Fix Rule Inputs** area, preview the fix commands that were previously defined in the policy, then click **Next**.

If custom policies are created with fix cli ^<Rule input ID>^ as the action for the condition, then the Fix Rule Inputs tab is displayed. Enter the required fix rule values and click **Next** to continue.

Step 7 Review the configuration that is displayed in the Preview Fix Commands pop up.

Step 8 Schedule the fix job so that the generated configuration can be deployed to the device, then Click **Schedule the Fix Job**.

What to do next

To view any of the violations job details, see [View Audit Failure and Violation Summary Details, on page 8](#).

View Audit Failure and Violation Summary Details

You can view detailed violation information, export this data, and view details of compliance jobs. You can export detailed data for a specific job, or export summary data for multiple jobs.

Step 1 Choose **Configuration > Compliance > Jobs**.

Step 2 To view the details for a specific audit job:

- a) Click the **Audit Jobs** tab and locate your job.
- b) Click the job's **Failure** hyperlink to view the **Compliance Audit Details** window.

You can view information about the policy name, the set rules, its compliance state, the total violation count, the job's instance count, its highest severity value, and the ignored count values.

- c) To export these details use one of the following options:
 - To export the violation details to a Microsoft Excel spreadsheet in XLS format, click **Export as XLS**.
 - To export the violation details to a Microsoft Excel spreadsheet in comma-separated text, click **Export as CSV**.
 - To export the violation details to an HTML file, click **Export as HTML**.
- d) Click **Save File**.

Step 3 To view a collective summary of all audit jobs:

- a) Click the **Violation Summary** tab.

You can view a collective report for all devices on which violations have occurred, their associated policy and profile names, their audit job IDs, their associated rules and rule severity values, details on whether the violations are fixable or not, or whether they are already fixed, and the message associated with the violation.

- b) To export this detailed summary report, choose one of the following options from the drop-down menu:
 - To export the summary to a Microsoft Excel spreadsheet in comma-separated text, click **Violation Report CSV**.
 - To export the summary to a PDF file, click **Violation Report PDF**.
- c) Click **Save File**.

What to do next

To fix any of the violations, see [Fix Device Compliance Violations, on page 9](#).

Import and Export Compliance Policies

Compliance policies are saved as XML files. You can export individual compliance policies and, if desired, import them into another server. Files can only be imported in XML format.

Step 1 Choose **Configuration > Compliance > Policies**.

Step 2 To export a compliance policy:

- a) Mouse hover on "i" icon next to the policy in the **Compliance Policies** navigation area on the left.
- b) In the popup window, click the **Export Policy as XML** hyperlink, and save the file.

Step 3 To import a compliance policy:

- a) Click the Import Policies icon above the **Compliance Policies** navigation area on the left.
 - b) In the **Import Policies** dialog box, click **Choose Policies**.
 - c) Browse to the XML file and select it.
 - d) Click **Import**.
-

View the Contents of a Compliance Policy XML File

Compliance policies are saved as XML files. To view the contents of a policy's XML file:

Step 1 Choose **Configuration > Compliance > Policies**.

Step 2 Locate the policy in the **Compliance Policies** navigation area on the left, then hover your mouse over the "i" icon next to the policy.

Step 3 In the popup window, click the **View Policy as XML** hyperlink. Cisco EPN Manager displays the content in XML format.

View PSIRT and EoX Information

- [View Device Security Vulnerabilities , on page 11](#)
- [View Device Hardware and Software End-of-Life Report , on page 12](#)
- [View Field Notices for Device , on page 12](#)

View Device Security Vulnerabilities

You can run a report to determine if any devices in your network have security vulnerabilities as defined by the Cisco Product Security Incident Response Team (PSIRT). The report includes Device PSIRT, Device Hardware EOX, Device Software EOX, and Field Notice information. You can also view documentation

about the specific vulnerabilities that describes the impact of a vulnerability and any potential steps needed to protect your environment.



Note PSIRT and EoX reports cannot be run for specific devices. When you schedule PSIRT and EoX jobs, the report is generated for all devices in Managed and Completed state (on the **Inventory > Configuration > Network Devices** page).

Before you begin

Sync the devices prior to scheduling the job. Choose **Configuration > Network Devices**, select the devices, then click **Sync**.

-
- Step 1** Choose **Reports > PSIRT and EoX**.
- Step 2** Schedule and run the job.
- A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, and Field Note information is gathered and reported. Separate jobs on each of the tabs need not be created.
- Step 3** Click **View Job Details** to view the current status of the PSIRT report.
- Step 4** When the report is completed, click the **Device PSIRT** tab to view PSIRT information.
- Step 5** In the **PSIRT Title** column, click the hyperlink to view the full description of a security vulnerability.
- Step 6** (Optional) You can export the device PSIRT details in PDF and CSV format for each device and for all devices collectively.
-

View Device Hardware and Software End-of-Life Report

You can run a report to determine if any Cisco device hardware or software in your network have reach edits end of life (EOX). This can help you determine product upgrade and substitution options.

-
- Step 1** Choose **Reports > PSIRT and EoX**.
- Step 2** Click **Schedule Job**. A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, and Field Note information is gathered and reported. You do not create separate jobs on each of the tabs.
- Step 3** After the job completes, click one of the following EOX tabs to view the report information specific to that tab:
- **Device Hardware EOX**
 - **Device Software EOX**
- Step 4** (Optional) You can export these device EoL details in PDF and CSV format for each device and for all devices collectively.
-

View Field Notices for Device

You can run a report to determine if any Cisco devices that are managed and have completed a full inventory collection have any field notices. Field Notices are notifications that are published for significant issues, other

than security vulnerability-related issues, that directly involve Cisco products and typically require an upgrade, workaround, or other customer action.

-
- Step 1** Choose **Reports > PSIRT and EoX**.
- Step 2** Click **Schedule Job**. A job is created in which Device PSIRT, Device Hardware EOX, Device Software EOX, and Field Note information is gathered and reported. You do not create separate jobs on each of the tabs.
- Step 3** Click the **Field Notice** tab to view field notice information.
- Step 4** Click on the hyperlink in the Field Notice Name column to view more information on cisco.com.
- Step 5** (Optional) You can export the device field notice details in PDF and CSV format for each device and for all devices collectively.
-

